AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph beginning on page 3, line 4 as follows:

Meanwhile, a mechanism called "key encapsulation mechanism" has recently been proposed as a new notion of the public-key cryptosystem (e.g. refer to the non-patent reference 3). This key encapsulation mechanism is an algorithm that enables distribution of a shared key between a transmission apparatus and a reception apparatus, using the public-key cryptosystem. In this mechanism, the transmission apparatus inputs a public key pk of a receiver into an encryption algorithm E, to generate a cipher text C and a shared key K, and transmits this cipher text C to the reception apparatus. Next, the reception apparatus inputs a secret key sk and the cipher text C into a decryption algorithm D, thereby obtaining the same shared key K ~~as~~ that the transmission apparatus owns.

Please amend the paragraph beginning on page 4, line 6 as follows:

With the key encapsulation mechanism, a transmitter cannot take a whole liberty with creation of a shared key, and therefore is prevented from committing fraud even though information is only allowed to be distributed from the transmitter to the receiver. This is the distinctive feature that the conventional arts do not have.

Please amend the paragraph on page 68, line 23 to page 69, line 6 as follows:

The first embodiment described above is one example of carrying out the present invention. Needless to say, the present invention is not limited to this particular embodiment, and can be carried out with various modifications as long as they are within the scope of the present invention. In light of this, the following cases are included in the present invention.

Please amend the paragraph beginning on page 69, line 7 as follows:

(1) The parameter N to be used in NTRU cryptosystem may take a value other ~~value~~ than 167.

Please amend the paragraph beginning on page 108, line 21 as follows:

As is clear from the above, the present invention provides a cryptosystem that the conventional technologies were not able to provide, and therefore is very valuable.